Summer SwA Working Group Sessions
June 28 - 30, 2011
MITRE, McLean VA

Tuesday June 28 – Plenary (Auditorium)

Session 1: Plenary – Joe Jarzombek, DHS, Don Davidson, DOD, and Mike Kass, NIST

- Welcome to the Software Assurance (SwA) Summer 2011 Working Group Session
- Review Goals and Objectives for this Working Group Session and the Spring Forum
- Overview of expectations
- SwA product gaps and updates
- What products do we have and what needs updating?

Break

Session 2: Plenary – Summary of US efforts – Joe Jarzombek, DHS, Don Davidson, DOD, Mike Kass and Jon Boyens, NIST (Invited)

The DHS paper "*Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action*" explores the idea of a healthy, resilient – and fundamentally more secure – cyber ecosystem of the future, in which cyber participants, including cyber devices, are able to work together in near-real time to anticipate and prevent cyber-attacks, limit the spread of attacks across participating devices, minimize the consequences of attacks, and recover to a trusted state. In this future cyber ecosystem, security capabilities are built into cyber devices in a way that allows preventive and defensive courses of action to be coordinated within and among communities of devices. Power is distributed among participants, and near-real time coordination is enabled by combining the innate and interoperable capabilities of individual devices with trusted information exchanges and shared, configurable policies.

Summary of UK Software Security, Dependability and Resilience Initiative (and related efforts) - Ian Bryant, MoD UK

In response to the 2010 UK National Security Strategy, which identified Cybersecurity as one of the four "Tier One" risks of particular concern, the UK has recently formed a public-private platform for enhancing the overall software and systems culture, with the objective that all software should become designed, implemented and maintained in a secure, dependable and resilient manner. This presentation explains the goals and structure of the new UK Software Security, Dependability and Resilience Initiative (SSDRI).

Discussion of Future Collaboration and opportunities for industry contribution

Lunch

Tuesday June 28 - Track A (Auditorium)

Session 3A: – Understanding Trends in SwA Adoption - Michele Moss and Stephanie Shankles, Booz Allen Hamilton

Recent industry reports have included analysis of trends in software assurance adoption. This session focus on enhancing the SwA Processes and Practices Working Group's understanding of the state of SwA and leveraging the insight from recent reports in Software Assurance outreach efforts.

Break

Session 4A: Software Engineering Institute (SEI) Community College Report - Nancy Mead, SEI

In this presentation, Volume IV of the Software Assurance Curriculum Project, the report on Community College Education, will be discussed. The report focuses on community college courses for software assurance and includes a review of related curricula, outcomes and body of knowledge, target audience, and outlines for six courses. By the time of the presentation at the Working Group meeting, this report will be available for review by the WET WG and other interested parties. The presentation will be given by Dr. Nancy R. Mead, Senior Researcher at CERT/SEI, and Technical Lead for the SwA Curriculum Project and the Build Security In website. Subsequent discussion will focus on additional WET WG activities that could be undertaken to reach out to and support community colleges and their faculty.

Tuesday June 28 - Track B (1H300)

Session 3B: Common Weakness Risk Analysis Framework (CWRAF) – Bob Martin and Steve Christey, MITRE, Richard Struse, DHS

In this session participants will construct one or more CWRAF "vignettes" for specific business domains. As each vignette is built and refined, we will automatically recalculate the scores for the entire CWE database, allowing participants to understand how the decisions made during vignette definition affect the assessment of risk for individual weaknesses. Input from attendees will be used to continue to refine the concepts in CWRAF and identify business domains and technology areas that would benefit from CWRAF.

Break

Session 4B: Using CWRAF to manage software risk in the Nuclear Power Industry – Richard Struse, DHS, and Eric Lee, NRC

This session will continue the themes established in Session 3B and will focus on a specific domain – Commercial Nuclear Power. Subject matter experts from the Nuclear Regulatory Commission will participate as we discuss how best to model risks arising from software weaknesses using CWRAF/CWSS for this domain.

Wednesday June 29 Track A (Auditorium)

Session 1A: Supply Chain Risk Management (SCRM) and SwA Standardization Updates – Don Davidson, DoD

This session will provide updates on current Supply Chain Risk Management (SCRM) and SwA standardization efforts to include (but not limited to) ISO 27036 & 15028, The Open Group's Trusted Technology Provider Framework (OTTPF) and NIST-IR 7622. Following these updates there will be audience discussion on where existing standards are currently being used, where new standards are needed and how emerging standards may fill gaps.

- Session Overview - Don Davidson, DOD – CIO
- Open Group progress on the O-TTPF - Andras Szakal, The Open Group
- Progress update on ISA efforts to develop guidance on securing electronic supply chains - Larry Clinton, ISA
- Contributions of Counterfeit standards to the management of sustainability and security in the lifecycle - TBD
- Update on NIST SwA and Supply Chain standards efforts - Jon Boyens, NIST (Invited)
- Update on ISO SwA and SCRM standards landscape – Nadya Bartol, Booz Allen Hamilton
- Questions and Discussion

Break

Session 2A: Specific, Measurable, Attainable, Realistic, and Timely (SMART) metrics: Identifying and Communicating Useful Metrics for IT Acquisition – Don Davidson, DoD, Thresa Lang, Dell, Suzanne Schwitalla, SOLE, and Nadya Bartol, Booz Allen Hamilton

The session will include an overview of the acquisition process, various stakeholders and information needs and existing measurement frameworks. (e.g., the Enterprise Risk Management Framework). Through a facilitated discussion, the Working Group will:

- Identify metrics and frameworks most commonly used
- Identify areas where standardized metrics could be more effective and efficient to acquisition personnel responsible for cross-enterprise purchases
- Identify gaps in current knowledge around the use of SMART metrics and how to address them.

The Working Group will discuss next steps for creating a state-of-the-practice guideline for the SwA community that can be leveraged across the IT vendor/supplier/user.

Lunch

Session 3A: Licensing and/or credentialing for software engineering – Dr. Candice Hoke, Cleveland State University

This session will explore the reasons, both pro and con, for licensing or other credentialing of developers. Dr. Candice Hoke, professor at the Cleveland-Marshall College of Law, will set the stage for a workshop discussion by enumerating the questions and issues that ineluctably follow if a decision were made to embrace licensing. By hearing the elements or questions that must be answered in order to produce an effective licensing scheme, the audience will be better enabled to make wise decisions as to whether this is a desirable path for enhancing SwA.

Dr. Hoke will chair a panel with Richard Marshall, DHS, Vehbi Tasar, ISC^2, Karen Evans, U.S. Cyber Challenge (Invited), and Jim Harper, CATO, to discuss not only the wisdom and efficacy of licensing with respect to SwA objectives, but also how various subsidiary questions might be answered if licensing were embraced (e.g., what type of governance organization and at what level (national or state- based); whether to require existing programmers to become licensed or instead apply only prospectively; whether certain educational programs will confer an automatic license, and many others).

Break

Session 4A: Workforce Education and Training (WET) – Mission, Goals and Planning - Dan Shoemaker, University of Detroit-Mercy, and Art Conklin, University of Houston

WET plans to develop detailed mission/purpose statement for the Working Group. The goal is to get an explicit definition of the boundaries and directions for this group beyond the statement on the website. Next WET will list, discuss, and prioritize long-term goals for the Working Group and define outcomes that would allow us to gauge whether we have met those goals. Suggested topics include:

- Development and agreement on direction of principles for a discipline of SwA
- Development of strategy for revising and then popularizing the CBK
- Development and agreement on directions for articulating SwA curriculum to conventional higher education applications
- Development of outreach strategy to community colleges
- Development of policy on licensure for the profession
- Definition of awareness mission

Next the Working Group will list, discuss, and prioritize its short-short term goals (e.g., for period preceding the Fall SwA Forum). The intent is to define outcomes that will allow us to gauge whether we have met those goals. Suggested topics include:

- Planning for integrating SwA with IA (role of CAEs) – this will be a hot topic at the CISSE board as well (from the direction of the CAEs)
- Planning for development of curriculum standard BOK (We have the reference curriculum – if we had the curricular standard to go with it we would have the complete set)
- Update-feedback on SwA Principles project – next steps
- Update-feedback on SwA Curriculum project – next steps

Wednesday June 29 - Track B (1H300)

Session 1B: Applications of the Common Weakness Enumeration

Helping Programmers Understand and Study Software Security Weaknesses: Semantic Templates – Robin Gandhi, University of Nebraska at Omaha

To cope with growing software complexity programmers need better mental models to sense the possibility of a vulnerability. There is no shortage of weakness enumerations and categorization but they are not in a form that facilitates human understanding and recall. For example, the CWE contains over 50 highly inter-related weakness definitions just to comprehend the possibility of buffer overflows. In this session, the development of Semantic Templates will be introduced for the study of software vulnerabilities. Work on Semantic Templates has been ongoing at the University of Nebraska Omaha since 2010. Using Semantic Templates experiments indicate a definite improvement in the programmer ability to understand the CWEs related to the underlying software fault, weakness characteristics, resources and locations affected and the consequences of a given CVE. Input from attendees will be used to guide the adoption of semantic template in education and research while soliciting avenues for further growth.

Software Fault Pattern - Djenana Campara, KDM Analytics

Software Fault Pattern (SFP) is a generalized description of an identifiable family of computations

- With formally defined characteristics
- With an invariant core and variant parts
- Fully discernable in code artifacts

Recently completed R&D project identified 36 SFPs covering space of 310 CWEs where CWEs are used as reporting mechanism. At this session we will discuss approach and outcome of this work. Break

Session 2B: Automation of Software Assurance

Software Assurance Findings Expression Schema (SAFES) and Tool Output Integration Format (TOIF) – Sean Barnum, MITRE, Djenana Campara, KDM Analytics, and Richard Struse, DHS

This session is targeted to software analysis tool providers and users, and will briefly describe the SAFES and TOIF representations. The goal of the session is to help attendees understand how these representations can enhance the value and usability of individual tools and enable tool users to significantly improve the depth of analysis they can perform. This session is also intended to answer specific questions on how to map existing tool representations to these common formats.

Software Assurance Visualization - Ken Prole and Hassan Radwan, AVI

Software Assurance Visualization aims to leverage existing tools by providing a framework for linking disparate testing and vulnerability analysis tools. Applied Visions, with DHS SBIR funding, will develop a visual analysis platform that embeds a mechanism for feedback from human analysis into automated analysis.

Lunch

Session 3B: CWE Enhancements

CWE Coverage Claims Representation (CCR) - Richard Struse, DHS

The CCR is a lightweight schema that allows a software analysis tool and/or service provider to state claims as to those CWEs that their technology or process can discover. This session is targeted to tool/service vendors and tool/service consumers with the goal of refining the CCR model for public release. Issues to be addressed include the specificity of claims, “anti-claims,” and key use-cases for CCR.

Toward CWE Compatibility Effectiveness - Paul E. Black, NIST

The Common Weakness Enumeration (CWE) defines a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that detect weaknesses in software. To encourage and recognize use of CWEs, MITRE has established the CWE Compatibility and Effectiveness Program.

Phases 1 and 2 of the program establish that tool warnings accurately map to CWEs. Phase 3 establishes which CWEs a tool (or capability) can identify and locate via testing. In this session, we propose (1) ideas on what constitutes acceptable fundamental and broad test sets for Phase 3, and (2) that the SAMATE Reference Dataset (SRD) be the repository and access for such test sets. Attendees will be asked to provide input and feedback on the following discussion points in the presentation:

- Programming languages for tests (which languages, standard vs. extended languages)
- Complexity of tests (high or low bar tests)
- Measuring capability effectiveness (complete or partial effectiveness)
- Test selection (real vulnerabilities vs. tests with weaknesses)
- Consideration of false-positive rate against capability effectiveness
- Need for countermeasures against "gaming" a test suite
- Repository features required to support test distribution

Break

Session 4B: Cyber Observables and CAPEC - Richard Struse, DHS, and Sean Barnum, MITRE

Cyber Observables eXpression (CybOX) - Use Cases

Exchange of meaningful information among cybersecurity data sources is a critical step on the path to effective automated defense against modern threats. How can we refine the open specifications so that event data and observable indicators may be parsed, filtered, and correlated by diverse families of cybersecurity systems in concert? What are the ways these standards could be leveraged by the community to better share automated network defense strategies? Attendees will be given a demonstration of a CybOX use case.

Common Attack Pattern Enumeration and Classification (CAPEC) Compatibility Program

This session will briefly describe the goals of a planned compatibility program for CAPEC and solicit input from the attendees on how the program should be designed and implemented to maximize its relevance to the community.

Thursday June 30 - Plenary (Auditorium)

Session 1: Security Automation and Software Assurance in the Cyber Ecosystem- Joe Jarzombek, DHS

In this session, representatives from the National Cyber Security Division of DHS will describe ongoing efforts within the Federal Government to leverage standards-based solutions to secure networks and systems. Specific topics will include CyberScope – an automated system for capturing information about department and agency FISMA compliance along with the emerging work on Continuous Monitoring.

Break

Session 2: Software Assurance Program Update - Joe Jarzombek, DHS, Don Davidson, DoD, Michael Kass, NIST

SwA Working Group (WG) Leaders will give 2-3 minute SwA Session Outbriefs on how this SwA WG week advanced their work plan, and where they need future work, ending up with discussion on each WG's Product Delivery Schedules. Next we will review and plan Outreach Events – 12 month past and 12 month future calendars – where have we been engaged, what's working, and where might we engage more.

Lunch

Session 3: SwA Performance Measures - Joe Jarzombek and Richard Struse, DHS

With increased concern for fiscal restraint, how should we measure performance and elicit management support? The DHS National Cyber Security Division (NCSD) SwA Program has articulated its goals, objectives, and measures. The current measures address capacity/capability and uptake. We are now considering effectiveness measures as well. During this session we will present an overview of existing SwA measures and solicit input from participants to refine and extend those measures.

Break

Session 4: SwA Forums and Working Groups – Planning for the Future – Joe Jarzombek, DHS, Don Davidson, DoD, Michael Kass, NIST

This session will outline the plans for upcoming Software Assurance Forums and Working Groups and engage the audience in a discussion focused on making these events as relevant and useful to attendees as possible. Discussion points will include: topics for future forums, suggestions for speakers, new perspectives to be addressed, and target audiences. Through a facilitated discussion, we will:

- Plan the agenda and calendar for 2011 Fall SwA Forum,
- Select major planning dates.
- Identify theme or major topics/speakers for the fall.
- Pick WG Products to be showcased this fall

Adjourn